UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/960,610	09/21/2001	Richard B. LeVine	ECD-0012	5654

7590 03/23/2006

Mills & Onello LLP
Suite 605
Eleven Beacon Street
Boston, MA 02108

EXAMINER	
MCKAY, KERRY A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/960,610	LEVINE ET AL.	
	Examiner	Art Unit	
	Kerry McKay	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/27/05*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-63, 85-133, and 155-160* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *See Continuation Sheet* is/are rejected.

7)☒ Claim(s) *10,17,24,27,28,31,42,51,54,55,58-61,88,97,104,113,114,117,128-131,158 and 160* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/22/02-5/31/05*. 7-2-03 4-12-04
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Continuation of Disposition of Claims: Claims rejected are 1-9,11-16,18-23,25,26,29,30,32-41,43-50,52,53,56,57,62,63,85-87,89-96,98-103,105-112,115,116,118-127,132,133,155-157 and 159.

DETAILED ACTION

1. This is a non-final action in response to communications filed December 27, 2005. The original claims, received September 21, 2001, contained claims 1-160, and was restricted. Applicant has elected group I, containing claims 1-63, 85-133, and 155-160. Claims 1-63, 85-133, and 155-160 are pending in this action.

Specification

2. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 3-7, 11-14, 20, 25, 26, 56, 57, 62, 63, 89-94, 98-101, 107, 111, 112, 126, 127, 132, 133, and 159 are rejected under 35 U.S.C. 102(e) as being anticipated by Reitmeier et al., US Patent Application Publication 2002/0003881 A1. Examiner

notes that corresponding prior art terms may accompany the claim language in bracketed form.

4. Regarding claim 1, Reitmeier et al. teach a method for preventing unauthorized use of digital content data comprising:

subdividing the digital content data into data segments ([0023]);

modifying the data segments with second data to generate modified data ([0029]); and

storing the modified data at predetermined memory locations ([0036]).

5. As per claim 56, Reitmeier et al. teach a method for preventing unauthorized use of digital content data hosted on a system comprising:

modifying the digital content data with saturation data to generate modified data ([0029]); and

storing the modified data at predetermined memory locations on the system to deter unauthorized access of the digital content data ([0036]).

6. Regarding claim 89, Reitmeier et al. disclose a system for preventing unauthorized use of digital content data comprising:

a subdividing unit (segmentation module) for subdividing the digital content data into data segments (figure 1, item 110A, [0023]);

a modification unit (re-sequencing module) for modifying the data segments with second data to generate modified data (figure 1, item 130, [0029]); and

a storage unit for storing the modified data at predetermined memory locations (figure 1, item 155, [0036]).

7. Regarding claim 126, Reitmeier et al. a system for preventing unauthorized use of digital content data hosted on a system comprising:
a modification unit for modifying the digital content data with saturation data to generate modified data (figure 1, item 130, [0029]); and
a storage unit for storing the modified data at predetermined memory locations on the system to deter unauthorized access of the digital content data (figure 1, item 155, [0036]).

8. Regarding claim 159, Reitmeier et al. teach a system for preventing unauthorized use of digital content data in a system having memory locations wherein the system enables a user to select from a plurality of tool modules, each module providing a service for protecting digital content from unauthorized use such that a user can protect digital content (figure 1, [0021], where the user (provider) has configuration options to choose from).

9. As per claim 3, the method of Reitmeier et al. teaches the method of claim 1 wherein the data segments are of a variable length ([0023]).

10. As per claim 4, the method of Reitmeier et al. teaches the method of claim 1 wherein the second data comprises a randomly generated data stream ([0029]).

11. As per claim 5, the method of Reitmeier et al. teaches the method of claim 1 wherein the second data comprises portions of the digital content data ([0029]).

12. As per claim 6, the method of Reitmeier et al. teaches the method of claim 1 further comprising encrypting the modified data and storing the encrypted modified data ([0036]).

13. As per claim 7, the method of Reitmeier et al. teaches the method of claim 6 further comprising encrypting the modified data with an encryption key ([0031], [0057]).

14. As per claim 11, the method of Reitmeier et al. teaches the method of claim 1 wherein the predetermined memory locations are selected as the locations at which the digital content data was originally stored ([0029], where Reitmeier et al. do not state that shuffling by a pseudo-random value cannot produce the original order).

15. As per claim 12, the method of Reitmeier et al. teaches the method of claim 1 wherein the digital content data comprises first and second digital content data and wherein the predetermined memory locations are selected as combinations of the

locations at which the first and second digital content data were originally stored ([0029]).

16. Regarding claim 13, the method of Reitmeier et al. teaches the method of claim 1 further comprising generating a map (index table) of locations at which the modified data is stored ([0018]).

17. As per claim 14, the method of Reitmeier et al. teaches the method of claim 13 further comprising storing the map of locations at the predetermined memory locations ([0018], [0036]).

18. As per claim 20, the method of Reitmeier et al. teaches the method of claim 1 further comprising:
retrieving the modified data from the predetermined memory locations; and
de-interleaving the data segments based on the second data to generate original digital content data (figure 4, [0046]).

19. As per claim 25, the method of Reitmeier et al. teaches the method of claim 1 wherein modifying the data segments comprises interleaving the data segments with the second data to generate interleaved data ([0057]).

20. As per claim 26, the method of Reitmeier et al. teaches the method of claim 1 wherein modifying the data segments with second data comprises tokenizing the data segments with token data ([0031], where Examiner interprets tokenizing as encryption in electronic codebook mode).

21. As per claim 57, the method of Reitmeier et al. teaches the method of claim 56 further comprising subdividing the digital content data into data segments and modifying the data segments ([0023]-[0029]).

22. As per claim 62, the method of Reitmeier et al. teaches the method of claim 56 further comprising interleaving the digital content data with second data to generate interleaved data ([0057]).

23. As per claim 63, the method of Reitmeier et al. teaches the method of claim 56 further comprising tokenizing the digital content data with token data (Reitmeier et al., [0031], where Examiner interprets tokenizing as encryption in electronic codebook mode).

24. As per claim 90, the system of Reitmeier et al. teaches the system of claim 89 wherein the data segments are of a variable length ([0023]).

25. As per claim 91, the system of Reitmeier et al. teaches the system of claim 89 wherein the second data comprises a randomly generated data stream ([0029]).

26. As per claim 92, the system of Reitmeier et al. teaches the system of claim 89 wherein the second data comprises portions of the digital content data ([0029]).

27. As per claim 93, the system of Reitmeier et al. teaches the system of claim 89 further comprising an encryption unit for encrypting the modified data and storing the encrypted modified data (figure 1, item 135, [0031]).

28. As per claim 94, the system of Reitmeier et al. teaches the system of claim 93 wherein the encryption unit further encrypts the modified data with an encryption key ([0031], [0057]).

29. As per claim 98, the system of Reitmeier et al. teaches the system of claim 89 wherein the predetermined memory locations are selected as the locations at which the digital content data was originally stored ([0029], where Reitmeier et al. do not state that shuffling by a pseudo-random value cannot produce the original order).

30. As per claim 99, the system of Reitmeier et al. teaches the system of claim 89 wherein the digital content data comprises first and second digital content data and wherein the predetermined memory locations are selected as combinations of the

locations at which the first and second digital content data were originally stored ([0029]).

31. As per claim 100, the system of Reitmeier et al. teaches the system of claim 89 further comprising a map generator for generating a map of locations at which the modified data is stored ([0018]).

32. As per claim 101, the system of Reitmeier et al. teaches the system of claim 100 wherein the storage unit further stores the map (index table) of locations at the predetermined memory locations ([0036]).

33. As per claim 107, the system of Reitmeier et al. teaches the system of claim 89 further comprising:
means for retrieving the modified data from the predetermined memory locations; and means for de-interleaving the data segments based on the second data to generate original digital content data (figure 4, [0046]).

34. As per claim 111, the system of Reitmeier teaches the system of claim 89 wherein the modification unit modifies the data segments comprises interleaving the data segments with the second data to generate interleaved data ([0057]).

35. As per claim 112, the system of Reitmeier et al. teaches the system of claim 89 wherein the modification unit modifies the data segments with second data comprises tokenizing the data segments with token data ([0031], where Examiner interprets tokenizing as encryption in electronic codebook mode).

36. As per claim 127, the system of Reitmeier et al. teaches the system of claim 126 further comprising subdividing the digital content data into data segments and modifying the data segments ([0023]-[0029]).

37. As per claim 132, the system of Reitmeier et al. teaches the system of claim 126 further comprising means for interleaving the digital content data with second data to generate interleaved data ([0057]).

38. As per claim 133, the system of Reitmeier et al. teaches the system of claim 126 further comprising means for tokenizing the digital content data with token data ([0031], where Examiner interprets tokenizing as encryption in electronic codebook mode).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

39. Claims 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier et al., US Patent Application Publication 2002/0003881 A1.

40. Regarding claim 2, the method of Reitmeier et al. teaches the method of claim 1 wherein the digital data comprises data types selected from a group consisting of audio, video ([0016]). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to extend protected data to documents, text and software, as they are digital content which is also susceptible to the same piracy concerns as audio and video, as stated in Applicant's description of the related art.

41. Claims 15, 16, 18, 19, 21-23, 29, 30, 32-39, 43-50, 52-53, 85-87, 102, 103, 105, 106, 108-110, 115, 116, 118-121, 123-125, and 155-157 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier et al., US Patent Application Publication 2002/0003881 A1, in view of Jensen et al., US Patent 5,930,828.

42. Regarding claim 29, Reitmeier et al. teach a method for preventing unauthorized use of digital content data in a system
having memory locations comprising:
subdividing the digital content data into data segments ([0023]);
modifying the data segments with second data to generate modified data ([0029]); and storing the modified data at the target memory locations ([0036]). Reitmeier et al. do not teach scanning or selecting memory locations.

Jensen et al. teach scanning the system to determine available memory locations and selecting target memory locations within the available memory locations at which to store data (column 12, lines 13-19, 27-31). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory scanning and targeting of Jensen et al. with the method of Reitmeier et al. to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

43. Regarding claim 85, Reitmeier et al. teach a method for preventing unauthorized use of digital content data in a system having memory locations comprising:
storing the digital content data at the target memory locations ([0036]). Reitmeier et al. do not teach scanning or selecting memory locations.

Jensen et al. teach scanning the system to determine available memory locations and selecting target memory locations within the available memory locations at which to store data (column 12, lines 13-19, 27-31). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory scanning and targeting of Jensen et al. with the method of Reitmeier et al.

to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

44. Regarding claim 115, Reitmeier et al. teach a system for preventing unauthorized use of digital content data in a system having memory locations comprising:
means for subdividing the digital content data into data segments (figure 1, item 110A, [0023];
means for modifying the data segments with second data to generate modified data (figure 1, item 130, [0029]); and
a storage unit for storing the modified data at the target memory locations (figure 1, item 155, [0036]). Reitmeier et al. do not teach means for scanning or a selector.

Jensen et al. teach means for scanning the system to determine available memory locations and a selector for selecting target memory locations within the available memory locations at which to store data (column 12, lines 13-19, 27-31). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory scanning means and selector of Jensen et al. with the system of Reitmeier to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

45. Regarding claim 155, Reitmeier et al. teach a system for preventing unauthorized use of digital content data in a system having memory locations comprising:
a storage unit for storing the digital content data at the target memory locations (figure 1, item 155, [0035], [0036]). The system of Reitmeier et al. does not teach a scanner or means for selecting target memory.

Jensen et al. teach a scanner and a means for selecting target memory locations within the available memory locations at which to store data (column 12, lines 13-19, 27-31). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory scanner and selecting means of Jensen et al. with the system of Reitmeier to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

46. Regarding claim 15, the method of Reitmeier et al. teaches the method of claim 1. Reitmeier et al. do not teach a scanning or selecting memory.

Jensen et al. teach scanning the system to determine available memory locations and selecting target memory locations within the available memory locations at which to store data (column 12, lines 13-19, 27-31). Jensen et al. further provide the motivation that this minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use

the memory scanning and selection of Jensen et al. with the method of Reitmeier et al. to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

47. As per claim 16, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 15 wherein a subset of available memory locations are located within file system locations (Jensen et al., column 3, lines 55-61).

48. As per claim 18, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 15 further comprising generating a map of the target memory locations (Jensen et al., column 12, lines 50-52).

49. As per claim 19, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 18 further comprising storing the map of target memory locations at the target memory locations (Jensen et al., column 12, lines 1-8, 41-44).

50. Regarding claim 21, the method of Reitmeier teaches the method of claim 1, wherein the memory locations reside on a system (figure 1, [0036]). The method of Reitmeier et al. does not teach a table of contents or a subset of memory locations between memory locations used by files.

Jensen et al. teach a table of contents (file allocation table) that identifies files stored on a system, wherein a subset of memory locations available for storing data are

between memory locations used by files stored on the system, as identified by the table of contents (figure 2B, column 6, lines 7-12). Jensen et al. further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the method of Reitmeier et al. in order to allow the operating system to locate files.

51. As per claim 22, the method of Reitmeier et al. teaches the method of claim 1. The method of Reitmeier et al. does not teach a table of contents that identifies files stored on a system.

Jensen et al. teach a table of contents (FAT) identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents (figure 2B, column 6, lines 7-12, where Examiner interprets free space as those locations in memory which are exclusive of files). Jensen et al. further provide the motivation that this table allows the operating system to locate files (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the table of Jensen et al. with the method of Reitmeier et al. to allow the operating system to locate files.

52. As per claim 23, the method of Reitmeier et al. teaches the method of claim 1. The method of Reitmeier et al. does not teach a table of contents that identifies files stored on a system.

Jensen et al. teach a table of contents (FAT) identifies files stored on the system, wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents (figure 7B, column 6, lines 7-12). Jensen et al. further provide the motivation that this table allows the operating system to locate files (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the table of Jensen et al. with the method of Reitmeier et al. to allow the operating system to locate files.

53. As per claim 30, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 wherein a subset of available memory locations are located within file system locations (Jensen et al., column 3, lines 55-61).

54. As per claim 32, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 further comprising generating a map of the target memory locations (Jensen et al., column 12, lines 50-52).

55. As per claim 33, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 32 further comprising storing the map of target memory locations at the target memory locations (Jensen et al., column 12, lines 1-8, 41-44).

56. As per claim 34, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 wherein the digital data comprises data types selected from a group consisting of audio, video ([0016]). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to extend protected data to documents, text and software, as they are digital content which is also susceptible to the same piracy concerns as audio and video, as stated in Applicant's description of the related art.

57. As per claim 35, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 wherein the data segments are of a variable length (Reitmeier et al., [0023]).

58. As per claim 36, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 wherein the second data comprises a randomly generated data stream (Reitmeier et al., [0029]).

59. As per claim 37, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 wherein the second data comprises portions of the digital content data (Reitmeier et al., [0029]).

60. As per claim 38, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 further comprising encrypting the modified data and storing the encrypted modified data (Reitmeier et al., [0036]).

61. As per claim 39, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 38 further comprising encrypting the modified data with an encryption key (Reitmeier et al., [0031], [0057]).

62. As per claim 43, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 wherein the predetermined memory locations are selected as the locations at which the digital content data was originally stored (Jensen et al., column 12, lines 46-49).

63. As per claim 44, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 wherein the digital content data comprises first and second digital content data and wherein the predetermined memory locations are selected as combinations of the locations at which the first and second digital content data were originally stored (Jensen et al., column 12, lines 46-49).

64. As per claim 45, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 further comprising generating a map of locations at which the modified data is stored (Jensen et al., column 6, lines 7-12).

65. As per claim 46, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 45 further comprising storing the map of locations at the predetermined memory locations (Jensen et al., column 12, lines 1-8, 41-44).

66. As per claim 47, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 further comprising:
retrieving the modified data from the predetermined memory locations; and
de-interleaving the data segments based on the second data to generate original digital content data (Reitmeier et al., figure 4, [0046]).

67. As per claim 48, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents (Jensen et al., figure 2, column 6, lines 7-12).

68. As per claim 49, the method of Reitmeier et l. and Jensen et al. teaches the method of claim 29 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations

of files stored on the system, as identified by the table of contents (figure 2B, column 6, lines 7-12, where Examiner interprets free space as those locations in memory which are exclusive of files).

69. As per claim 50, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents (Jensen et al., column 6, lines 7-12).

70. As per claim 52, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 wherein modifying the data segments comprises interleaving the data segments with the second data to generate interleaved data (Reitmeier et al., [0057]).

71. Regarding claim 53, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 29 wherein modifying the data segments with second data comprises tokenizing the data segments with token data (Reitmeier et al., [0031], where Examiner interprets tokenizing as encryption in electronic codebook mode).

72. As per claim 86, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 85 wherein a subset of available memory locations are located within files identified by the file system locations (Jensen et al., figure 2B, column 6, lines 7-12, where clusters may be scattered and fragmented, allowing the memory locations to be within the range of the first and final cluster of the files).

73. As per claim 87, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 85 wherein a subset of available memory locations are located between files identified by the file system locations (Jensen et al., figure 2B, column 6, lines 7-12, column 12, lines 13-16).

74. Regarding claim 102, the system of Reitmeier et al. teaches the system of claim 89. Reitmeier et al. do not teach a scanner or selector.

Jensen et al. teach scanning the system to determine available memory locations and selecting target memory locations within the available memory locations at which to store data (column 12, lines 13-19, 27-31). Jensen et al. further provide the motivation that this minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory scanner and selector of Jensen et al. with the system of Reitmeier et al. to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

75. As per claim 103, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 102 wherein a subset of available memory locations are located within file system locations (Jensen et al., column 3, lines 55-61).

76. As per claim 105, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 102 further comprising a map generator for generating a map of the target memory locations (Jensen et al., column 12, lines 50-52).

77. As per claim 106, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 105 wherein the storage unit stores the map of target memory locations at the target memory locations (Jensen et al., column 12, lines 1-8, 41-44).

78. Regarding claim 108, the system or Reitmeier et al. teaches the system of claim 89. The system of Reitmeier et al. does not teach a table of contents that identifies files stored on a system.

Jensen et al. teach a table of contents (FAT) identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents (figure 2B, column 6, lines 7-12). Jensen et al. further provide the motivation that this table allows the operating system to locate files (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention

to use the table of Jensen et al. with the system of Reitmeier et al. to allow the operating system to locate files.

79. As per claim 109, the system of Reitmeier et al. teaches the system of claim 89. The system of Reitmeier et al. does not teach a table of contents that identifies files stored on a system.

Jensen et al. teach a table of contents (FAT) identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents (figure 2B, column 6, lines 7-12, where Examiner interprets free space as those locations in memory which are exclusive of files). Jensen et al. further provide the motivation that this table allows the operating system to locate files (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the table of Jensen et al. with the system of Reitmeier et al. to allow the operating system to locate files.

80. As per claim 110, the system of Reitmeier et al. teaches the system of claim 89. The system of Reitmeier et al. does not teach a table of contents that identifies files stored on a system.

Jensen et al. teach a table of contents (FAT) identifies files stored on the system, wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents (figure 2B, column 6, lines 7-12). Jensen et al. further

provide the motivation that this table allows the operating system to locate files (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the table of Jensen et al. with the system of Reitmeier et al. to allow the operating system to locate files.

81. As per claim 116, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 115 wherein a subset of available memory locations are located within file system locations (Jensen et al., column 3, lines 55-61).

82. As per claim 118, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 115 further comprising a map generator for generating a map of the target memory locations (Jensen et al., column 12, lines 50-52).

83. As per claim 119, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 118 wherein the storage unit stores the map of target memory locations at the target memory locations (Jensen et al., column 12, lines 1-8, 41-44).

84. As per claim 120, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 115 further comprising means for encrypting the modified data and wherein the storage unit stores the encrypted modified data (Reitmeier et al., figure 1, item 135, [0031], [0036]).

85. As per claim 121, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 120 wherein the means for encrypting further encrypts the modified data with an encryption key (Reitmeier et al., [0031], [0057]).

86. As per claim 123, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 115 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents (Jensen et al., figure 2B, column 6, lines 7-12).

87. As per claim 124, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 115 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents (Jensen et al., column 6, lines 7-12, where Examiner interprets free space as those locations in memory which are exclusive of files).

88. As per claim 125, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 115 wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at

which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents (Jensen et al., column 6, lines 7-12).

89. As per claim 156, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 155 wherein a subset of available memory locations are located within files identified by the file system locations (Jensen et al., figure 2B, column 6, lines 7-12, where clusters may be scattered and fragmented, allowing the memory locations to be within the range of the first and final cluster of the files).

90. As per claim 157, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 155 wherein a subset of available memory locations are located between files identified by the file system locations (Jensen et al., figure 2B, column 6, lines 7-12, column 12, lines 13-16).

91. Claims 8-9 and 95-96 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier et al., US Patent Application Publication 2002/0003881 A1, in view of Schneier, "Applied Cryptography", pages 176-177.

92. Regarding claim 8, the method of Reitmeier et al. teaches the method of claim 7. The method of Reitmeier et al. does not teach encrypting the encryption key.

Schneier teaches key distribution by encrypting an encryption key (data key) with a key-encrypting key (page 176, section 8.3, paragraph 3). Schneier further provides the motivation that this allows two parties, Alice and Bob, to distribute data keys often without allowing an eavesdropper to gain knowledge of the data encryption keys (pages 176-177, section 8.3. It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the data key distribution method of Schneier to transmit the data key from the provider to the subscriber in the method Reitmeier et al., allowing the subscriber to decrypt the encrypted data.

93. As per claim 9, the method of Reitmeier et al. and Schneier teaches the method of claim 8 further comprising storing the encryption key with the encrypted modified data at the predetermined memory locations (Reitmeier et al., [0036], where the system must also possess the decryption key in order to decrypt the encrypted data).

94. As per claim 95, the system of Reitmeier et al. teaches the system of claim 94. The method of Reitmeier et al. does not teach encrypting the encryption key.

Schneier teaches key distribution by encrypting an encryption key (data key) with a key-encrypting key (page 176, section 8.3, paragraph 3). Schneier further provides the motivation that this allows two parties, Alice and Bob, to distribute data keys often without allowing an eavesdropper to gain knowledge of the data encryption keys (pages 176-177, section 8.3. It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the data key distribution of Schneier to transmit the

data key from the provider to the subscriber in the system Reitmeier et al., allowing the subscriber to decrypt the encrypted data.

95. As per claim 96, the system of Reitmeier et al. and Schneier teaches the system of claim 95 wherein the storage unit further stores the encryption key with the encrypted modified data at the predetermined memory locations (Reitmeier et al., [0036], where the system must also possess the decryption key in order to decrypt the encrypted data).

96. Claims 40, 41, and 122 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reitmeier et al., US Patent Application Publication 2002/0003881 A1, and Jensen et al., US Patent 5,930,828, in further view of Schneier, "Applied Cryptography", pages 176-177.

97. Regarding claim 40, the method of Reitmeier et al. and Jensen et al. teaches the method of claim 39. The method of Reitmeier et al. and Jensen et al. does not teach encrypting the encryption key.

Schneier teaches key distribution by encrypting an encryption key (data key) with a key-encrypting key (page 176, section 8.3, paragraph 3). Schneier further provides the motivation that this allows two parties, Alice and Bob, to distribute data keys often without allowing an eavesdropper to gain knowledge of the data encryption keys (pages 176-177, section 8.3. It would have been obvious to one of ordinary skill in the art at the

time of Applicant's invention to use the data key distribution of Schneier to transmit the data key from the provider to the subscriber in the method Reitmeier et al. and Jensen et al., allowing the subscriber to decrypt the encrypted data.

98. As per claim 41, the method of Reitmeier et al., Jensen et al., and Schneier teaches the method of claim 40 further comprising storing the encryption key with the encrypted modified data at the predetermined memory locations (Reitmeier et al., [0036], where the system must also possess the decryption key in order to decrypt the encrypted data).

99. Regarding claim 122, the system of Reitmeier et al. and Jensen et al. teaches the system of claim 121. The system of Reitmeier et al. and Jensen et al. does not teach encrypting the encryption key.

Schneier teaches key distribution by encrypting an encryption key (data key) with a key-encrypting key (page 176, section 8.3, paragraph 3). Schneier further provides the motivation that this allows two parties, Alice and Bob, to distribute data keys often without allowing an eavesdropper to gain knowledge of the data encryption keys (pages 176-177, section 8.3. It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the data key distribution of Schneier to transmit the data key from the provider to the subscriber in the system Reitmeier et al. and Jensen et al., allowing the subscriber to decrypt the encrypted data.

Allowable Subject Matter

100. Claims 10, 17, 24, 27, 28, 31, 42, 51, 54, 55, 58-61, 88, 97, 104, 113, 114, 117, 128-131, 158, and 160 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

101. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

102. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kerry McKay whose telephone number is (571) 272-2651. The examiner can normally be reached on Monday-Friday, 8:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KM
03/17/06

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100